VU VRIJE UNIVERSITEIT AMSTERDAM

VU Research Portal

Evaluatie en toekomst van de Wet bescherming persoonsgegevens

de Vries, H.H.

published in
Computerrecht
2010

Link to publication in VU Research Portal

citation for published version (APA)
de Vries, H. H. (2010). Evaluatie en toekomst van de Wet bescherming persoonsgegevens. *Computerrecht*, *2010*(4), 173-180.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:
vuresearchportal.ub@vu.nl

Download date: 04. May. 2023

Mw. mr. Hester de Vries

Evaluatie en toekomst van de Wet bescherming persoonsgegevens

103

De evaluatie van de Wet bescherming persoonsgegevens toont aan dat de bescherming van persoonsgegevens tekort schiet. Er is sprake van gebrekkige normontwikkeling, onverschilligheid van betrokkenen ten aanzien van de bescherming van persoonsgegevens, nalevingtekort van de wettelijke verplichtingen door de verantwoordelijken en onvoldoende middelen voor de toezichthouder om de naleving van wettelijke verplichtingen af te dwingen. Waar de evaluatie een somber beeld schetst van het beschermingsniveau in Nederland, wordt op Europees niveau de lat van het beschermingsniveau hoger gelegd. Wat betekent dit voor de toekomst van de wetgeving ter bescherming van persoonsgegevens in Nederland?

1. Bescherming van persoonsgegevens – tijd voor bezinning

In november 2009 verscheen het kabinetsstandpunt over het rapport van de Commissie veiligheid en persoonlijke levenssfeer en de evaluatie van de Wet bescherming persoonsgegevens[1] (hierna WBP). De evaluatie van de WBP, die gefaseerd werd uitgevoerd, toont aan dat de bescherming van persoonsgegevens tekort schiet. Het kabinet beoogt in het licht van de evaluatie van de WBP 'een nieuwe benadering voor de bescherming van persoonsgegevens'. Er zal een concreet wetsvoorstel worden ingediend tot wijziging van de WBP, naast het wetsvoorstel tot vermindering van een aantal administratieve lasten en nalevingslasten dat op dit moment al bij de Tweede Kamer in behandeling is.[2] Het klinkt veelbelovend, maar als gevolg van de val van het kabinet is het wetsvoorstel controversieel verklaard.[3] Dit betekent dat moet worden afgewacht welke standpunten het nieuwe kabinet zal innemen en of de behandeling spoedig zal kunnen worden voortgezet. Toch is er geen reden om nu achterover te leunen. Op Europees niveau is namelijk de voorbereiding van de evaluatie van de Richtlijn bescherming persoonsgegevens in gang gezet.[4] Op 1 december 2009 publiceerde de Artikel 29 Werkgroep al het rapport 'The Future of Privacy'[5] en de Nederlandse regering heeft in het kader van de openbare consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de Europese Unie haar standpunt bekend gemaakt.[6]

Een goed moment voor bezinning op de toekomstige bescherming van persoonsgegevens. Immers, waar eerder discussie over sommige knelpunten in de WBP werd gesmoord in het dwingende kader van de Richtlijn bescherming persoonsgegevens, lijkt nu enige bewegingsruimte te ontstaan. Of er ruimte zal zijn voor versoepeling van het normenkader valt echter te betwijfelen. Terwijl in Nederland de evaluatie van de WBP een somber beeld schetst van het beschermingsniveau en een trage poging wordt ondernomen om de administratieve lasten en nalevingskosten van de WBP te verminderen, wordt op Europees niveau de lat van het beschermingsniveau hoger gelegd, zodat naar verwachting de nalevingskosten in de toekomst eerder hoger dan lager zullen uitvallen.

2. Evaluatie van de WBP

De evaluatie van de Wet bescherming persoonsgegevens vloeit voort uit de wettelijke opdracht in art. 80 WBP. De evaluatiebepaling is met name opgenomen om te bewaken of de WBP in de pas loopt met de snelle technologische ontwikkelingen. 'Bezien zal moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer ontoereikend garanderen.'[7] Conform art. 80 WBP diende het rapport van de evaluatie binnen vijf jaar na de inwerkingtreding van de wet, dus voor 1 september 2006 aan de Staten-Generaal te worden gezonden. Die termijn is niet gerealiseerd. De

1. Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Stb.* 2000, 302 in werking getreden op 1 september 2001. Laatstelijk gewijzigd per 1 juli 2009, *Stb.* 2009, 265.
2. Wetsvoorstel Wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen, *Kamerstukken II* 2008/09, 31 841, nr. 2.
3. *Kamerstukken II* 2009/10, 32 333, nr. 20, p. 3.
4. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Zie verder de consultatie inzake de herziening van het juridische raamwerk voor de bescherming van persoonsgegevens in de Europese Unie. *http://ec.europa.eu.*
5. Article 29 Data Protection Working Party, Working Party on Police and Justice *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, 2009.
6. Op de website van de Europese Commissie zijn 168 standpunten die zijn ingezonden gepubliceerd, waaronder ook het standpunt van de Nederlandse regering. Zie *http://ec.europa.eu.*
7. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 197.

evaluatie van de WBP is gefaseerd uitgevoerd.[8] De eerste fase van de evaluatie betrof een literatuuronderzoek en knelpuntenanalyse; de tweede fase empirisch onderzoek dat voortborduurt op de in de eerste fase geconstateerde knelpunten. Het rapport van de eerste fase van de evaluatie verscheen in 2007, het rapport van de tweede fase van de evaluatie in 2009.

Dat de naleving van de WBP knelpunten oplevert voor de praktijk, was al duidelijk voordat de evaluatie werd gestart. Zo heeft het College bescherming persoonsgegevens (hierna CBP) al op 7 december 2004 tien voorstellen gedaan voor reductie van de administratieve lasten op grond van de WBP.[9] Op 12 juli 2005 heeft het CBP nog een aantal aanvullende voorstellen gedaan om de administratieve lasten te verminderen.[10] Toch duurde het geruime tijd, namelijk tot het voorjaar van 2009[11], voordat op basis van deze voorstellen een concreet voorstel van wet tot wijziging van de WBP werd ingediend. Dit wetsvoorstel staat los van de evaluatie van de WBP, maar loopt vanwege de traagheid van het wetgevingsproces inmiddels parallel met de officiële evaluatie van de WBP. Bij herhaling is toegezegd dat het wetsvoorstel inzake de administratieve lasten geen eindstation is, en dat er in reactie op de evaluatie van de WBP separaat een wetsvoorstel zal worden ingediend.

2.1. *Conclusies evaluatie WBP*

In het rapport over de eerste fase van de evaluatie wordt vanuit juridisch perspectief gewezen op de belangrijkste knelpunten die voortvloeien uit de moeizame aansluiting van de WBP bij het Nederlandse rechtssysteem. In de eerste plaats is volgens de onderzoekers het gelaagde en gecompartimenteerde systeem voor de bescherming van persoonsgegevens bijzonder complex geworden. Het tendeert soms zelfs naar overregulering. Daar komt bij dat het begrippenapparaat en instrumentarium van de WBP als zodanig te abstract zijn en te veel ruimte laten voor interpretatie om een helder kader te vormen voor de beoordeling van concrete vragen en situaties. Daarmee wordt de doelstelling van het vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen niet (ten volle) gerealiseerd.

In de tweede plaats wijzen de onderzoekers vanuit het perspectief van de handhaving en de naleving op het eenzijdig karakter van de handhaving. Daarnaast krijgt het beoogde stelsel van checks en balances maar beperkt vorm door het gebrek aan feitelijke rechterlijke toetsing van de beginselen van de WBP. De doelstellingen van de rechterlijke toetsing van de aan het CBP toegekende bevoegdheden en de nadere invulling van de materiële normen via zelfregulering, zijn maar beperkt gerealiseerd.

In de derde plaats valt vanuit het perspectief van de beeldvorming en bekendheid op dat veel rechten en plichten van verantwoordelijken en betrokkenen die voortvloeien uit de WBP, niet optimaal worden uitgeoefend door een gebrek aan bekendheid van deze rechten en plichten. Een van de centrale doelstellingen van de WBP, namelijk het vergroten van de transparantie van gegevensverwerking door de toekenning van rechten en plichten en het instellen van een toezichthouder lijken daarmee (ten dele) onverwezenlijkt.[12]

In het rapport over de tweede fase, het empirisch onderzoek, concluderen Winter e.a. dat 'de doelstellingen van de WBP, het waarborgen van evenwicht tussen het privacybelang en andere grondrechten en het versterken van de positie van personen van wie gegevens worden verwerkt, nog niet ten volle worden gerealiseerd'.[13] Uit enquêteonderzoek, interviews en case studies komt het beeld naar voren van een wet die in de rechtspraktijk nog niet erg leeft, betrekkelijk lastig hanteerbaar wordt geacht en waarbij een op de toepassing gerichte privacygemeenschap en -cultuur nog niet in de volle breedte tot ontwikkeling is gekomen.

2.2. *Beleving van de betrokkene*

Afgezien van de 'officiële' evaluatierapporten die hun grondslag vinden in art. 80 WBP, zijn diverse onderzoeksrapporten verschenen die bijdragen aan de verslaglegging 'over de doeltreffendheid en de effecten' van de WBP in de praktijk. Zo liet het CBP in 2009 een onderzoek uitvoeren naar de beleving van betrokkenen; de individuen om wie het bij bescherming van persoonsgegevens per slot van rekening te doen is. De onderzoekers concluderen in het rapport 'Niets te verbergen en toch bang' dat burgers als het gaat om verstrekking van persoonsgegevens een meegaande houding vertonen. De veronderstelling dat deze houding zou voortkomen uit de gedachte niets te verbergen te hebben, wordt echter door het onderzoek niet bevestigd. Het gedrag van burgers moet volgens de onderzoekers eerder worden beoordeeld in termen van

8. Ook de evaluatie van de voorganger van de WBP, de Wet Persoonsregistraties, werd gefaseerd uitgevoerd. De juridische evaluatie werd verricht door G. Overkleeft-Verburg in haar dissertatie. Zie G. Overkleeft-Verburg, *De Wet persoonsregistraties, norm, toepassing en evaluatie*, Zwolle: Tjeenk Willink, 1995. De sociaal wetenschappelijke evaluatie werd verricht onder leiding van J.E.J. Prins, *In het licht van de Wet persoonsregistraties: zon, maan of ster?*, Alphen a/d Rijn: Samsom, 1995.
9. Deze voorstellen zijn afgestemd met de Commissie Privacy van de Raad van de Centrale Ondernemingsorganisaties. Brief van het CBP aan de Minister van Justitie, 7 december 2004, z2004-1086.
10. Brief van het CBP aan de Minister van Justitie, 12 juli 2005, z2004-1494.
11. *Kamerstukken II* 2008/09, 31 841, nr. 2.
12. G. Zwenne, A. Duthler, M. Groothuis, H. Kielman, W. Koelewijn en L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag: WODC 2007, p. 176.
13. H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg, H. Prakken, *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: WODC 2008, p. 157.

een gevoel van onvermijdelijkheid en gelatenheid dan in termen van vertrouwen in een correct gebruik van de gegevens. De onderzoekers concluderen dat de burgers onvoldoende op de hoogte zijn van mogelijke risico's die zijn verbonden aan het delen en verwerken van persoonsgegevens. Opvallend is overigens dat burgers als het gaat om een zorgvuldige verwerking van gegevens, meer vertrouwen hebben in de overheid dan in het bedrijfsleven.[14]

3. Privacy en veiligheidsdomein – een bijzonder aandachtsgebied

De kabinetsreactie inzake de evaluatie van de WBP van 3 november 2009[15] ziet niet alleen op de (officiële) evaluatierapporten, maar ook en in het bijzonder, op het rapport van de Adviescommissie Veiligheid en persoonlijke levenssfeer, de Commissie-Brouwer-Korf.[16] Het laatste rapport wordt in de kabinetsreactie zelfs voorop gesteld, en dat lijkt symbolisch voor de (overwegende) invloed die het rapport op de kabinetsreactie lijkt te hebben gehad.[17]
Op zichzelf is dat niet onbegrijpelijk: niet alleen is het rapport van de Commissie-Brouwer-Korf relatief kort voor de standpuntbepaling van het kabinet gepubliceerd, op het moment waarop de andere rapporten wellicht al enigszins aan actualiteit verloren leken te hebben, maar bovendien heeft het rapport van de Commissie-Brouwer-Korf een sterk politieke lading. Centraal in het rapport staat het spanningsveld tussen privacy en veiligheid. Een onderwerp dat bewust buiten het bereik van de 'gewone' evaluatie van de WBP is gebracht.[18]

Sinds de vrees voor terroristische aanslagen greep heeft gekregen op westerse samenlevingen, wordt regelmatig de stelling betrokken dat privacy zou moeten wijken voor het veiligheidsbelang. Alsof het beperken van de privacyrechten van burgers zonder meer zou leiden tot een betere veiligheid. De Commissie heeft oog voor deze vermeende tegenstelling van belangen en komt tot de conclusie dat privacy en veiligheid niet zonder elkaar kunnen: er moet gewoon een afweging gemaakt worden tussen veiligheid en privacy. We moeten vooral niet krampachtig doen om beide belangen zoveel als in concrete situaties mogelijk is, recht te doen. De Commissie draagt daartoe een Richtinggevend kader aan. Dit kader borduurt voort op de beginselen van gegevensbescherming, die inmiddels bijna dertig jaar geleden door de OESO zijn aangenomen[19] en die nog steeds een veilige basis vormen voor een zorgvuldige gegevensverwerking. De Commissie zet uiteen dat het Richtinggevend kader beoogt de rationaliteit te versterken van de beslissing of men een bepaalde verwerking van persoonsgegevens wel of niet zou moeten willen. Daartoe brengt het de spanning die er kan zijn tussen veiligheid en privacy in beeld en faciliteert het kader het nadenken over de diverse te maken afwegingen.[20]

Uiteindelijk lijkt de Commissie toch voorrang te geven aan het veiligheidsbelang: indien de veiligheid daartoe noodzaakt, *moeten* persoonsgegevens gedeeld worden.[21] De Commissie wil dit uitgangspunt expliciteren in art. 9 WBP over 'niet onverenigbaar gebruik'. Mijns inziens draagt de Commissie hier een oplossing aan die naar haar aard niet past binnen het kader van de WBP. De WBP biedt immers een stelsel van normen voor behoorlijke en zorgvuldige verwerking van persoonsgegevens, maar bevat geen normen die *verplichten* tot gegevensverwerking. Voor zover een *verplichting* tot gegevensverwerking aan de orde zou zijn, hoort deze mijns inziens thuis in sectorspecifieke wet- of regelgeving, niet in de WBP.

4. Knelpunten en toekomstperspectief

Het ligt voor de hand dat knelpunten die zijn geanalyseerd in het kader van de evaluatie van de WBP bepalend (of in ieder geval medebepalend) zullen zijn voor de toekomstige ontwikkeling van de WBP. En het ligt ook voor de hand dat de ontwikkelingen op nationaal en op Europees niveau elkaar wederzijds zullen beïnvloeden. Het kabinet heeft aangekondigd dat het in het licht van de evaluatie van de WBP 'een nieuwe benadering voor de verwerking van persoonsgegevens', voorstaat, gebaseerd op een viertal kernthema's, namelijk: het versterken van de waarborgen bij de omgang met persoonsgegevens; robuust extern toezicht; minder nadruk op procedures

14. J. Koffijberg, S. Dekkers, G. Homburg en B. van den Berg, *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan, 2009.
15. *Kamerstukken II* 2009/10, 31 051, nr. 5, Brief van de Ministers van Justitie en van Binnenlandse Zaken aan Voorzitter van de Tweede Kamer der Staten-Generaal.
16. Het rapport is te raadplegen op *www.veiligheidbegintbijvoorkomen.nl*.
17. Dit werd ook opgemerkt tijdens de behandeling van het kabinetsstandpunt door de Vaste Kamercommissie voor Justitie op 3 februari 2010. Zie *Kamerstukken II* 2009/10, 31 051, nr. 7, p. 2.
18. Zie Zwenne e.a., 2007, p. 18.
19. Zie de *Guidelines on the protection of privacy and transborder flow of personal data*, OECD 1980. Parijs 1981). Zie ook het Europees Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 1981, *Trb.* 1988, 7. Verdrag 108 van de Raad van Europa. In het najaar van 2010 vinden diverse bijeenkomsten plaats in het kader van de verjaardag van de Richtlijnen, die vervolgens in 2011 zullen worden geëvalueerd.
20. Het Richtinggevend kader bestaat uit zes grondslagen met bijbehorende handreikingen in de vorm van een stappenplan: 1. Transparantie, tenzij; 2. Selecteer voor je verzamelt en houd het sober ('select before you collect'); 3. Indien nodig voor de veiligheid moet je delen; 4. Zorg voor integriteit van gegevens, systemen en het handelen van gebruikers; 5. Zorg voor voorlichting en facilitering; 6. Zorg voor naleving en intern toezicht. Commissie-Brouwer-Korf, 2009.
21. 'Door duidelijk te maken dat – als aan de noodzakelijke randvoorwaarden is voldaan – gegevens *moeten* worden gedeeld kunnen instellingen en instanties die niet willen delen zich niet langer achter privacywetgeving verschuilen'. Aldus Commissie-Brouwer-Korf, 2009, toelichting op grondslag 3. Volgens Dommering is hier sprake van een onderschikking van privacy aan veiligheid. Zie E. Dommering, 'Privacy als zelfbeschikkingsrecht van de 21e eeuw', *Mediaforum* 2009, 11/12, p. 383. Zie ook H. Buitelaar en C. Cuijpers, 'De balans tussen veiligheid en privacy. Kanttekeningen bij het standpunt van het kabinet', *NJB* 2009, p. 2820-2824.

en controle vooraf; versterking van de positie van de burger.[22] Het kabinet meent dat deze kernthema's ook de grondslagen van de Richtlijn bescherming persoonsgegevens raken en heeft de kernthema's om die reden ook onder de aandacht gebracht van de Europese Commissie. Het kabinet bepleit een betere uitwisseling van informatie indien dat nodig is voor de veiligheid en meer waarborgen bij de omgang met persoonsgegevens, ondersteund door stevige handhaving, ook buiten het terrein van de veiligheid. De Artikel 29 Werkgroep en de Werkgroep Politie en Justitie stellen zich in het rapport 'The Future of Privacy' op het standpunt dat de basisbeginselen voor gegevensbescherming nog steeds waarde hebben, ook in het licht van de ontwikkeling van nieuwe technologieën en globalisering, maar doen eveneens een aantal voorstellen voor wijziging van de Richtlijn bescherming persoonsgegevens. Hieronder schets ik in vogelvlucht een aantal van de voorstellen die zouden moeten bijdragen aan de totstandkoming van een nieuwe benadering voor de verwerking van persoonsgegevens.

4.1. *Werkingssfeer en toepassing van de WBP*

Het eerste en belangrijke door Zwenne e.a. gesignaleerde knelpunt van de WBP betreft de reikwijdte van deze wet. Er is veel kritiek op de onduidelijkheid en onbepaaldheid of algemeenheid en alomvattendheid van de wettelijke begrippen, zoals persoonsgegeven, verantwoordelijke, bewerker en derde.[23] De kabinetsreactie gaat aan dit wezenlijke knelpunt, zonder nadere toelichting, voorbij, vermoedelijk omdat de definities rechtstreeks voortvloeien uit de Richtlijn bescherming persoonsgegevens en er op dit punt geen ruimte is voor nationale afwijking.

In het rapport 'The future of privacy' wordt evenmin aandacht besteed aan het begrippenkader, maar wordt verwezen naar rapporten van de Artikel 29 Werkgroep die inmiddels een nadere toelichting heeft gegeven op de definities van 'persoonsgegeven', 'verantwoordelijke' en 'verwerker'.[24] Duidelijk is dat het begrip 'persoonsgegeven' zeer ruim wordt uitgelegd, en steeds verder afdrijft van de kerngedachte van eerbiediging van de persoonlijke levenssfeer. Meer en meer gegevens die op het eerste gezicht niet met een persoon van doen hebben, zoals het IP-adres van een computer en een cookie op een computer, worden als volwaardige persoonsgegevens aangemerkt. Het feit dat een derde partij over de middelen beschikt om deze gegevens met een persoon in verband te brengen, maakt dat dezelfde gegevens ook in handen van andere partijen kwalificeren als persoonsgegevens. 'Bescherming van persoonsgegevens', ook aangeduid met het foeilelijke Anglicisme 'dataprotectie', ontwikkelt zich tot een zelfstandig rechtsdomein, nauw verwant aan, maar niet langer een onlosmakelijk onderdeel van het rechtsdomein 'privacy'. Deze ontwikkeling komt tot uitdrukking in de zelfstandige plaats die 'bescherming van persoonsgegevens' als op zichzelf staand grondrecht, naast het grondrecht op privacy, heeft gekregen in het Handvest van de grondrechten van de Europese Unie.[25]

Het wordt mijns inziens evenwel tijd voor bezinning op een nadere classificatie van gegevens, met een bijbehorend beschermingsniveau. Naast de categorieën 'persoonsgegeven' en 'bijzonder persoonsgegeven' waarvoor een strikter beschermingsregime geldt, zou een derde categorie kunnen worden onderscheiden van beschermwaardige gegevens, waarop vooralsnog slechts een selectie van de wettelijke normen van toepassing is.[26] Dergelijke beschermwaardige gegevens, (of 'bijna persoonsgegevens'), zoals het hiervoor genoemde IP-adres en de cookie in gevallen waarin degene die deze gegevens verwerkt zelf niet over de middelen beschikt om deze met een natuurlijke persoon in verband te brengen, zouden bijvoorbeeld wel onderworpen zijn aan de algemene beginselen van behoorlijke en zorgvuldige gegevensverwerking, transparantie en beveiliging. Op het moment waarop de desbetreffende gegevens daadwerkelijk persoonsgegevens zijn geworden, dient het 'normale' wettelijke regime van toepassing te zijn. Mijns inziens is een nadere classificatie van (persoons)gegevens en differentiatie in het beschermingsregime niet alleen wenselijk met het oog op de naleving en de handhaafbaarheid van de wettelijke verplichtingen, maar ook om veilig te stellen dat gegevens die naar hun aard meer bescherming verdienen, deze ook daadwerkelijk krijgen. Een te grote reikwijdte van het wettelijke kader brengt mijns inziens het risico van erosie van de bescherming met zich mee. Overigens meent ook het kabinet dat 'zich op de langere termijn' de noodzaak zal aandienen voor een meer fundamentele verandering van de betekenis van een aantal basisbegrippen uit de Richtlijn. Het kabinet verwijst naar verschijnselen als 'cloud computing' en 'Radio frequency identification'. Omdat het eindbeeld van deze ontwikkelingen nog onzeker is, is het naar het oordeel van het

22. *Kamerstukken II* 2009/10, 31 051, nr. 1, p. 6.
23. Zwenne e.a., 2007, p. 61-65.
24. Groep Gegevensbescherming Artikel 29, *Advies 4/2007 over het begrip persoonsgegeven*, WP 136, 2007 en *Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'*, WP 169, 2009. De Artikel 29 Werkgroep spreekt van ' verwerker', en bedoelt daarmee de partij die in de WBP is aangemerkt als bewerker.
25. Art. 7 van het Handvest (Eerbiediging van het privéleven en het familie- en gezinsleven) bepaalt: Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie. Art. 8 (Bescherming persoonsgegevens) bepaalt: 1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens. 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels. Voor een toelichting zie bijv. P. Hustinx, 'The relation between transparency and the rights of privacy and the protection of personal data', Seminar *Transparency and Clear Legal Language in the EU*, Swedish Presidency, Stockholm, 8 September 2009.
26. Zie ook J. Terstegge, 'Is het privacyrecht klaar voor de toekomst', *Tijdschrift voor Internetrecht* 2008, nr. 3, p. 65-66. Hij pleit ervoor om verschillende privacylagen te onderscheiden, ieder met een eigen wettelijk beschermingsregime.

kabinet echter onmogelijk om nu al vastomlijnde standpunten in te nemen.[27]

Afgezien van de centrale begrippen in de WBP is ook de territoriale werkingssfeer van de WBP onderwerp van kritiek. De in art. 4 WBP verankerde regel dat de wet van toepassing is op 'een verwerking van persoonsgegevens in het kader van een vestiging van de verantwoordelijke in Nederland' blijkt voor meerdere uitleg vatbaar te zijn. Het CBP heeft op enig moment het standpunt ingenomen dat de WBP (slechts) van toepassing is als *de verantwoordelijke* zelf in Nederland is gevestigd. Voor de toepasselijkheid van de WBP zou geen aanleiding zijn als alleen een vestiging van de verantwoordelijke in Nederland is gevestigd.[28] Analyse van de totstandkoming van de Richtlijn bescherming persoonsgegevens wijst uit dat deze interpretatie niet juist is. De Europese Commissie heeft uitdrukkelijk beoogd dat een verantwoordelijke met vestigingen in meerdere lidstaten, in ieder van die lidstaten moet voldoen aan het ter plaatse geldende recht, indien verwerking van persoonsgegevens plaatsvindt in het kader van de activiteiten van deze vestigingen.[29] Inmiddels lijkt het CBP het eerdere omstreden standpunt te hebben herzien.[30] De regel van art. 4 leidt echter tot een onnodige cumulatie van verplichtingen op grond van het lokaal toepasselijke recht in de verschillende lidstaten voor verantwoordelijken met meerdere vestigingen in de EU.[31] Het is wenselijk dat daarvoor op Europees niveau een oplossing wordt gevonden. De Artikel 29 Werkgroep heeft op dit moment een rapport over toepasselijk recht in voorbereiding[32] dat mogelijk nieuwe oplossingen zal aandragen. In ieder geval lijkt nadere uitwerking van het beginsel van privacygovernance en accountability, waarop ik hieronder (in § 4.3) nader zal ingaan, een aanknopingspunt voor oplossing van het probleem van toepasselijk recht.

4.2. ***Het normatieve kader***

Zwenne e.a. wijzen allereerst op het probleem dat op grond van de WBP lastig is vast te stellen wie als verantwoordelijke moet worden aangemerkt en op wie derhalve de verplichtingen op grond van de WBP rusten. Dit speelt met name in grotere organisaties waar het feitelijk beheer van en verantwoordelijkheid voor informatiesystemen niet altijd duidelijk is. Het probleem speelt ook in situaties waar verschillende partijen met elkaar samenwerken en bijvoorbeeld ook bij verwerkingen van persoonsgegevens via het internet. De kabinetsreactie gaat voorbij aan dit knelpunt. De Artikel 29 Werkgroep heeft inmiddels een nadere toelichting gegeven op de reikwijdte en onderlinge afstemming van de begrippen 'verantwoordelijke' en 'bewerker'. De SWIFT-zaak leerde al dat een partij die formeel als bewerker is aangewezen, maar in de praktijk de bevoegdheid heeft (genomen) om beslissingen te nemen over verwerkingen van persoonsgegevens, toch als verantwoordelijke voor de gegevensverwerking wordt aangemerkt.[33] Terecht kan een verantwoordelijke zich niet aan zijn wettelijke verplichtingen onttrekken, door zich contractueel te verschuilen achter een andere partij.[34]

Een volgend door Zwenne e.a. gesignaleerd knelpunt betreft de vaagheid van de materiële wettelijke normen, die bovendien zouden vergen dat iedere verwerking opnieuw daaraan wordt getoetst. Alleen specialisten zouden in staat zijn tot toepassing van de open wettelijke normen (doelbinding, noodzaak, 'niet onverenigbaar gebruik'). De vaagheid van de wettelijk normen brengt onder meer het risico mee, dat privacy het excuus wordt om verwerkingen te verhinderen, omdat deze op grond van de WBP niet zouden zijn toegestaan.[35] Om het spanningsveld tussen veiligheid en privacy te doorbreken, stelt het kabinet in navolging van de Commissie-Brouwer-Korf een Richtinggevend kader voor.[36] Daarnaast stelt het kabinet stelt voor om (specifiek voor het overheidsdomein) een helpdesk in te richten die de professional kan assisteren om de juiste afwegingen te maken.[37] In de literatuur en ook bij de behandeling van de kabinetsreactie in de Vaste Kamercommissie van Justitie zijn hierover terecht kritische opmerkingen gemaakt: niet valt in te zien waarom de professional binnen de overheid zou moeten worden geassisteerd bij de belangenafweging,

27. Zie *http://ec.europa.eu*.
28. Zie M.A.H. Fontein-Bijnsdorp, 'Artikel 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wbp', *Computerrecht* 2008, 168, p. 285-289. Dit artikel is een reactie op het artikel van E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008, 61. Zwenne merkt op dat de reactie van mevr. Fontein, senior beleidsmedewerker bij het CBP, niet 'op persoonlijke titel' is geschreven en dus kennelijk het standpunt van het CBP verwoord. Zie G-J. Zwenne en G.C.J. Erents, 'Reikwijdte Wbp: enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp', *Privacy & Informatie* 2009, 2, p. 60-67.
29. Zie de tekst van art.4 lid 1 onder a van de Richtlijn bescherming persoonsgegevens 'wanneer dezelfde verantwoordelijke een vestiging heft op het grondgebied van verscheidene Lid-Staten, dient hij de nodige maatregelen te treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving'. Zie verder het artikel van E.M.L. Moerel, 'Art. 4 revisited'; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008, 169.
30. Op de site van het CBP staat de volgende tekst over toepasselijk recht: 'Heeft een verantwoordelijke meerdere vestigingen in de Europese Unie, dan dient hij ervoor zorg te dragen dat elk van de vestigingen voldoet aan de regels van het land waar de vestiging zich bevindt.' Zie *http://www.cbpweb.nl*.
31. De Nederlandse regering wijst hier op in haar inbreng in de consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de EU. Zie *http://ec.europa.eu*.
32. Naar verwachting verschijnt dit rapport in het najaar van 2010.
33. Groep gegevensbescherming artikel 29, *Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank* Financial Telecommunication (SWIFT), WP 128, 2006, p. 11-13.
34. Groep gegevensbescherming artikel 29, WP 169.
35. Zie Zwenne e.a., 2007, p. 45 e.v., Commissie-Brouwer-Korf, 2009, uitleg bij grondslag 3 (p. 50 e.v.).
36. *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 11-21. Zie ook noot 24.
37. *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 21.

maar het bedrijfsleven, dat evenzeer worstelt met het wettelijke kader, niet.[38]

Het kabinet kondigt overigens aan dat de normen op een aantal punten kunnen worden geconcretiseerd. Voorbeelden zijn de invoering van een Privacy Impact Assessment); bevorderen van Privacy by Design (zodat de bescherming van persoonsgegevens direct in het ontwerp van systemen wordt ingebouwd, denk aan 'privacy default settings' bij gebruik van bijvoorbeeld internetdiensten); eventuele sanctionering van onvoldoende naleving van de beveiligingsverplichting; een verplichting om de bewaartermijn van gegevens te motiveren dan wel een opschoonverplichting; en last but not least de invoering van een meldplicht in geval van (ernstige) doorbraken van beveiligingsmaatregelen.[39]

Veel van de genoemde voorstellen worden ook genoemd in het rapport 'The Future of Privacy'. Een wettelijke meldplicht datalekken zal binnen afzienbare termijn in ieder geval worden ingevoerd in de telecommunicatiesector, nu de gewijzigde e-Privacy Richtlijn daartoe verplicht.[40] In verschillende EU-lidstaten en met name in de Verenigde Staten is ervaring opgedaan met een dergelijke meldplicht.[41] Het blijkt van groot belang om vooraf het beoogde doel van de meldplicht scherp te formuleren: gaat het er primair om de betrokkenen in staat te stellen om eventuele schade als gevolg van doorbraak van de beveiliging te beperken? Of (ook) om de betrokkenen in staat te stellen tot het indienen van een schadeclaim? Of gaat het louter om transparantie rond beveiligingsdoorbraken? Dienen alle doorbraken te worden gemeld of alleen doorbraken ten aanzien van bijzondere persoonsgegevens? Of alleen doorbraken waar het risico van schade bestaat? Bij welke instantie moet worden gemeld? Op welke wijze moet worden gemeld (schriftelijk?; in dagbladen?; op internet?)? En wordt aan de meldplicht een sanctie gekoppeld? En zo ja, waarop wordt de sanctie dan gebaseerd (achterwege laten van een melding/of vaststelling dat beveiliging is doorbroken)? Op 15 april 2010 werd een eerste versie van het voorstel van wet tot wijziging van de Telecommunicatiewet voor consultatiedoeleinden gepubliceerd.[42] Conform dit voorstel zal gemeld moeten worden aan de OPTA. Dit heeft geleid tot een kritische reactie van het CBP, dat, omdat reeds het voornemen bestaat om de meldplicht uit te breiden tot partijen buiten de telecommunicatiesector, zich op het standpunt stelt dat een meldplicht richting CBP de voorkeur verdient.[43]

4.3. *Zelfregulering*

Als knelpunt op het terrein van zelfregulering noemen Zwenne e.a. de beperkte totstandkoming van de Gedragscodes, mede in verband met de wijze waarop het CBP invulling geeft aan de goedkeuringsbevoegdheid. Daarnaast noemen zij als knelpunt de positie van de Functionaris voor de Gegevensbescherming (hierna FG). Op grond van art. 62 WBP kan een verantwoordelijke of een organisatie waarbij verantwoordelijken zijn aangesloten overgaan tot benoeming van een FG. De FG wordt in de WBP primair voorgesteld als een alternatief voor de meldingsplicht richting het CBP; wanneer een FG is aangesteld, kan de verantwoordelijke de gegevensverwerking melden aan de FG, in plaats van het CBP. Knelpunt vormt onder meer de afbakening van bevoegdheden tussen de FG en het CBP.[44]

Het kabinet is van mening dat zelfregulering op grond van de WBP bevorderd dient te worden. Verplicht voorschrijven van een FG binnen organisaties is blijkens de kabinetsreactie niet aan de orde. Het kabinet onderschrijft wel het belang van het benoemen van functionarissen die toezien op de naleving van privacywaarborgen, omdat dit een positieve uitwerking zou kunnen hebben op het niveau van gegevensbescherming. Intern toezicht wordt door het kabinet, mijns inziens terecht, een 'onderschat instrument' genoemd.[45] Het kabinet meent dat de WBP de ruimte zou kunnen bieden om bedrijven of instellingen meer vrijheid te bieden ten opzichte van de wettelijke verplichtingen (zoals vrijstelling van de meldingsplicht of vrijstelling van de verplichting om een voorafgaand onderzoek aan te vragen) wanneer deze organisaties een eigen privacybeleid vaststellen en bekendmaken, en een FG of een daarmee op één lijn te stellen functionaris aanwijzen.

Privacygovernance is het woord waarmee de beoogde inbedding van privacycompliance in organisaties wordt samengevat. Ook in het rapport 'The Future of Privacy' wordt het belang ervan benadrukt onder de klassieke

38. *Kamerstukken II* 2009/10, 31 051, nr. 7, p. 2. Buitelaar en Cuijpers stellen: 'De voorgestelde helpdesk vormt een prachtig voorbeeld van een instrument waarin zowel bij wet als in de praktijk reeds was voorzien in de vorm van het College bescherming persoonsgegevens (CBP).' De beoogde helpdesk ter compensatie van de terugtrekkende rol van het CBP is te elfder ure ingesteld. Zie H. Buitelaar en C. Cuijpers, 2009, p. 2822.
39. *Kamerstukken II* 2009/10, 31 051, nr. 5. Zie ook de inbreng van de Nederlandse regering in de consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de EU. *http://ec.europa.eu*.
40. Conform art. 2 van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonl?ke levenssfeer in de sector elektronische communicatie en verordening (EG) nr. 2006/2004 betreffende samenwerking met betrekking tot consumentenbescherming (*PbEG* L 337).
41. M.H. Wugmeister en C.J. Rich, 'Breach notification legislation. Key elements to consider', April 2010, paper for *Forum on International Privacy Law*, Geneva.
42. Zie *www.internetconsultatie.nl*.
43. Wetgevingsadvies CBP inzake wijziging van de Telecommunicatiewet 4 juni 2010, z2010-00475.
44. Zwenne e.a., 2007, p. 79-80.
45. Zie *http://ec.europa.eu*.

term 'accountability'. Accountability of privacygovernance lijkt de oplossing te bieden voor het gebrek aan naleving van de verplichtingen op grond van de WBP. Het gaat om het beheersbaar maken van de naleving van de wettelijke verplichtingen, zodat daarover expliciet verantwoording kan worden afgelegd. Het is mijns inziens verstandig dat het kabinet de bevordering van privacygovernance ziet in samenhang met versoepeling van wettelijke verplichtingen en niet introduceert als een nieuwe, concrete wettelijke verplichting. In het rapport 'The Future of Privacy' wordt de mogelijkheid van versoepeling van verplichtingen ook genoemd, maar wordt niet uitgesloten dat 'accountability' dwingend wordt voorgeschreven.

Wie de naleving van de nu geldende wettelijke verplichtingen serieus neemt, zal de facto de meeste onderdelen van privacygovernance hebben gerealiseerd.[46] Nieuw is evenwel het aspect van *aantoonbaar* maken van de naleving; een concept waarmee de toezichthouders binnen de Europese Unie de afgelopen jaren ervaring hebben opgedaan in het kader van de goedkeuring van Binding Corporate Rules. De bouwstenen van de BCR's vormen ook de bouwstenen van privacygovernance. Naast de invulling van de materiële wettelijke normen, het toesnijden van de wettelijke normen op de gegevensverwerking binnen de organisatie van de verantwoordelijke, in de vorm van privacybeleid en bindende, heldere richtsnoeren en werkinstructies voor alle medewerkers, gaat het vooral ook om het invoeren van mechanismen om de uitvoering van het beleid, de richtsnoeren en werkinstructies te bewaken. Daarbij kan worden gedacht aan de uitvoering van privacy impact assessments; regelmatig uitvoeren van audits om de naleving in de praktijk te controleren; het geven van opvolging aan audits, invoering van een klachtenregeling, training van mensen en zorgvuldige verslaglegging. Het intern delegeren van verantwoordelijkheden, dat wil zeggen het aanwijzen van personen die kunnen worden aangesproken op de naleving van de wet- en regelgeving en het beleggen van het toezicht op de naleving van de regels is onderdeel van privacygovernance. Daarnaast gaat het ook om het beheersbaar maken van gegevensstromen naar en bescherming door externe partijen (bewerkers en andere ontvangers van gegevens).

Aan de inrichting en instandhouding van privacygovernance hangt uiteraard wel een prijskaartje. Het is de vraag hoe deze prijs zich verhoudt met het streven in Nederland om de administratieve lasten en nalevingskosten van de WBP terug te dringen. Het is mijns inziens van groot belang dat van meet af aan rekening wordt gehouden met de schaal waarop de verwerkingen plaatsvinden: de grootte van de organisatie van de verantwoordelijke; de omvang van de gegevensverwerking en de impact van de gegevensverwerking voor betrokkenen zijn onder meer criteria om af te wegen hoe zwaar de privacygovernance op de organisatie zal dienen te drukken.[47]

4.4. *Transparantie en rechten van betrokkenen*

Transparantie omvat de meldplicht van de gegevensverwerking en de informatieplicht richting betrokkenen. Het nut en de toegevoegde waarde van de meldplicht van gegevensverwerkingen wordt door Zwenne e.a. als knelpunt genoemd. In het kader van het wetsvoorstel tot wijziging van de WBP in verband met terugdringen van de administratieve lasten heeft het kabinet al aangekondigd dat de vrijstelling van de meldplicht zal worden verruimd.[48] Nog niet duidelijk is hoe de verruiming van de vrijstellingen zich zal verhouden tot het hierboven beschreven beginsel van privacygovernance. Wellicht kan de meldplicht worden beperkt tot een eenvoudige melding bij het CBP van naam en adres van de verantwoordelijke.[49]

Ook de invulling van de informatieplicht richting betrokkenen en de uitoefening van de rechten door betrokkenen worden door Zwenne e.a. als knelpunt genoemd.[50] Het kabinet stelt een aantal maatregelen voor om de transparantie van de gegevensverwerking voor burgers te verbeteren. Op de website *www.burgerservicenummer.nl* kunnen burgers bijvoorbeeld nagaan welke organisaties welke gegevens uitwisselen met behulp van het burgerservicenummer en op de website *www.mijnoverheid.nl* kunnen burgers zien welke informatie bij overheidsorganisaties over hen bekend is. Ook buiten de overheidssector wenst het kabinet de invulling van de informatieplicht te verbeteren, bijvoorbeeld op het punt van verstrekking van informatie over profilering. Daarnaast wil het kabinet het privacybewustzijn van burgers vergroten: zij zijn per slot van rekening zelf verantwoordelijk voor eigen keuzes bijvoorbeeld ten aanzien van de verstrekking van persoonsgegevens. Klachtenregelingen zouden voorts een bijdrage kunnen leveren aan het versterken van de positie van betrokkenen.

In het rapport 'The Future of Privacy' worden ook andere voorstellen gepresenteerd. Zo wordt opgemerkt dat nieuwe manieren moeten worden ontwikkeld om betrokkenen te informeren, bijvoorbeeld in het kader van behavioural targeting. Ook wordt een algemene informatieplicht in het kader van datalekken voorgesteld. Daarnaast wordt uiteengezet dat 'toestemming' van de betrokkene als grondslag voor de verwerking van per-

46. Overigens kan men zich ook de vraag stellen of privacy compliance niet al deel zou moeten zijn van normaal corporate governance, zeker in het geval privacyrisico's een wezenlijk bestandsdeel zijn van de bedrijfsrisico's.

47. Article 29 Data Protection Working Party, Working Party on Police and Justice, WP 168, 2009, p. 20.

48. *Kamerstukken II* 2008/09, 31 841, nr. 3, p. 3.

49. Article 29 Data Protection Working Party, Working Party on Police and Justice, WP 168, 2009, p. 16 e.v.

50. Zwenne e.a., 2007, p. 126-127. Winter e.a. concluderen dat het blijkt dat betrokkenen niet vaak gebruik maken van de formele bevoegdheden die de WBP biedt om de regie over hun gegevens te voeren. Winter e.a., 2008, p. 82 e.v.

soonsgegevens verduidelijking behoeft in de nieuwe regeling: impliciete toestemming voor verwerking van persoonsgegevens op het internet kwalificeert niet zonder meer als ondubbelzinnige toestemming. Meer in het algemeen meent de Artikel 29 Werkgroep dat de positie van betrokkenen in verband met het internet in de gewijzigde Richtlijn verduidelijkt moet worden.[51] Daarbij moet ook aandacht zijn voor een verdere harmonisering van de bepalingen, omdat bepalingen die essentieel zijn voor de bescherming van de betrokkenen op dit moment op zeer verschillende wijze door de lidstaten zijn geïmplementeerd als gevolg waarvan de positie van de betrokkenen wordt ondermijnd.

4.5. *Toezicht en rechtsbescherming*

Zwenne e.a. concluderen dat over de WBP betrekkelijk weinig wordt geprocedeerd, waardoor onzekerheid blijft bestaan over de invulling en concretisering van veel open normen in de wet.[52] Over de vraag of het CBP voldoende of te weinig bevoegdheden heeft blijkt verschillend te worden gedacht.[53] De Commissie-Brouwer-Korf spreekt zich duidelijk uit voor robuust extern toezicht en handhaving van de WBP.[54] Ook het kabinet en de Artikel 29 Werkgroep spreken zich uit voor versterken van de bevoegdheden van de toezichthouder.[55] De Artikel 29 Werkgroep constateert dat er grote verschillen bestaan tussen de bevoegdheden van de toezichthouders in de 27 lidstaten en meent dat de nieuwe uitdagingen op het terrein van gegevensbescherming sterk toezicht vereisen, op een meer uniforme en effectieve wijze. Toezichthouders moeten volledig onafhankelijk zijn en beschikken over voldoende middelen. In de toekomst zou de Richtlijn meer uniformiteit moeten bieden op het punt van de bevoegdheden van toezichthouders. Als noodzakelijke bevoegdheid van de toezichthouders wordt uitdrukkelijk genoemd de bevoegdheid om financiële sancties op te leggen aan verantwoordelijken en bewerkers.

Het versterken van de handhavingbevoegdheden van de toezichthouder is mijns inziens een noodzakelijke stap om naleving van de WBP te bevorderen. Het samenstel van maatregelen, waaronder de stimulering van privacygovernance, de inbedding van privacybescherming in organisaties en in het bijzonder het aantoonbaar maken van compliance vereenvoudigt de handhavingstaken van de toezichthouder aanzienlijk. Een punt van zorg blijft evenwel het open karakter van de wettelijke normen, waardoor een verantwoordelijke het risico loopt (blijft lopen) dat achteraf gezien de gegevensverwerking naar het oordeel van de toezichthouder niet (in alle opzichten) aan de WBP voldoet. Het kabinet meent dat aan dit bezwaar voldoende tegemoet kan worden gekomen door de publicatie van richtsnoeren voor de gegevensverwerking door het CBP.[56] Het kabinet merkt op dat de richtsnoeren uiteraard wel voldoende concreet moeten zijn, op zorgvuldige wijze moeten worden voorbereid en tijdig bekend moeten worden gemaakt. En daar zit mijns inziens precies het probleem; gedurende het proces van de ontwikkeling van systeemarchitectuur en inrichting van de gegevensverwerking kunnen in de praktijk nieuwe vragen opkomen, die de toezichthouder niet had kunnen bedenken, en waarop binnen het kader van de open wettelijke normen verschillende antwoorden denkbaar zijn, die bovendien vaak snel moeten worden gegeven. Om die reden mag van het CBP coulance worden verwacht bij toezicht en handhaving op basis van zorgvuldig ingerichte privacygovernance. Wanneer onverhoopt naar het oordeel van de toezichthouder toch sprake zou zijn van schending van wettelijke normen, zou eerst tijd en ruimte geboden moeten worden voor verbetering, voordat een hard oordeel wordt openbaar gemaakt en een sanctie wordt opgelegd.

5. Conclusie

De evaluatie van de WBP biedt inzichten in de knelpunten van het wettelijke systeem gericht op de bescherming van persoonsgegevens. Het totaalbeeld stemt somber, maar de conclusie dat de basisbeginselen voor gegevensbescherming hun waarde hebben behouden, biedt ook kansen voor verdere ontwikkeling. Bescherming van persoonsgegevens ontwikkelt zich tot een nieuw rechtsgebied verwant aan, maar niet langer een onlosmakelijk onderdeel van het privacyrecht. De kabinetsreactie op de evaluatie van de WBP en het rapport van de Commissie-Brouwer-Korf omvat een aantal voorstellen voor verbetering, met name uitwerking van de grondbeginselen, inbedding van de bescherming van persoonsgegevens in organisaties, robuuste handhaving en versterking van de positie van betrokkenen, die nauw aansluiten op de voorstellen gepresenteerd in het rapport 'The Future of Privacy' van de Artikel 29 Werkgroep. Op een versoepeling van de wettelijke normen hoeft niet gerekend te worden; naar verwachting zal de wijziging van de Richtlijn juist meer en concrete verplichtingen tot naleving omvatten, die hun weg zullen vinden naar de Wet bescherming persoonsgegevens.

51. Article 29 Data Protection Working Party, Working Party on Police and Justice, WP 168, 2009, p. 18.
52. Zwenne e.a., 2007, p. 88.
53. Zwenne e.a., 2007, p. 85.
54. 'Robuust toezicht betekent: 'op basis van een scherpe prioritering de feitelijke omgang met persoonsgegevens op de werkvloer aan toezicht onderwerpen. (...) Dat wil zeggen: niet volstaan met beoordelen of de papieren werkelijkheid van codes en reglementen strookt met de wettelijke verplichtingen. Dat brengt ook mee: niet alléén op basis van signalen reageren, maar ook op basis van eigen prioritering proactief de praktijk induiken om bij te dragen aan de wisselwerking tussen praktijk, regels en de belangen en waarden die in de regels zijn vervat." Commissie-Brouwer-Korf, 2009.
55. *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 26-29. Zie ook de inbreng van de Nederlandse regering in de consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de EU, *http://ec.europa.eu*. Article 29 Data Protection Working Party, Working Party on Police and Justice, WP 168, 2009, p. 21-23.
56. *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 28.